STIC Search Report

EIC 2100

STIC Database Tracking Number: 164312

TO: Nadia Khoshnoodi Location: RND 2 B 65 Art Unit: 2133 Tuesday, August 30, 2005 Case Serial Number: 09683943	**From: Emory Damron** Location: EIC 2100 RND 4B19 Phone: 571-272-3520 Emory.Damron@uspto.gov

Search Notes

Dear Nadia,

Please find below your fast and focused search.
References of potential pertinence have been tagged, but please review all the packets in case you like something I didn't.
Of those references which have been tagged, please note any manual highlighting which I've done within the document.
In addition to searching on Dialog, I also searched EPO/JPO/Derwent, and AltaVista.
There may be a few decent references contained herein, but I'll let you determine how useful they may be to you.
Please contact me if I can refocus or expand any aspect of this case, and please take a moment to provide any feedback (on the form provided) so EIC 2100 may better serve your needs. Good Luck!

Sincerely,
Emory Damron
Technical Information Specialist
EIC 2100, US Patent & Trademark Office
Phone: (571) 272-3520
Emory.damron@uspto.gov
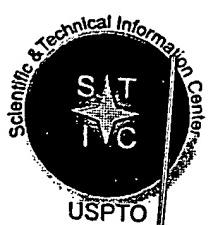
STIC EIC 2100
Search Request Form

Today's Date 8/20/05

What date would you like to use to limit the search?
Priority Date: 3/7/2001   Other:

Name Nadia Khoshnoodi

AU 2133   Examiner # 80432

Room # 2 B65   Phone 2-3825

Serial # 09/683943

Format for Search Results (Circle One):
(PAPER)   DISK   EMAIL

Where have you searched so far?
USP DWPI EPO JPO ACM IBM TDB
IEEE INSPEC SPI   Other _____

Is this a "Fast & Focused" Search Request? (Circle One) (YES) NO
A "Fast & Focused" Search is completed in 2-3 hours (maximum). The search must be on a very specific topic and meet certain criteria. The criteria are posted in EIC2100 and on the EIC2100 NPL Web Page at http://ptoweb/patents/stic/stic-tc2100.htm.

What is the topic, novelty, motivation, utility, or other specific details defining the desired focus of this search? Please include the concepts, synonyms, keywords, acronyms, definitions, strategies, and anything else that helps to describe the topic. Please attach a copy of the abstract, background, brief summary, pertinent claims and any citations of relevant art you have found.

*digital safe deposit accounts associated w/ 1 private key

(in an environment of ATM processing)

generating digital signature from private key

*COPY

P6PUB/2002/0129256

STIC Searcher Emory Damico   Phone 2-3520
Date picked up 8/30/05   Date Completed 8/30/05

sira
Search and Information
Resources Administration

```
Set       Items    Description
S1        65291    ACCOUNT?
S2       2328196   SAFEDEPOSIT? OR SAFE?()DEPOSIT? OR SAFETYDEPOSIT? OR ELECT-
                   RONIC? OR FINANCIAL? OR CHECKING? OR SAVINGS? OR DEBIT OR CRE-
                   DIT? OR BANK?
S3        5969     AUTOMAT?()TELLER?
S4          18     (DRIVE(')UP OR DRIVE()THRU OR DRIVEUP OR DRIVETHRU)(2N)(BAN-
                   K? OR TELLER?)
S5        42368    ATM OR ATMS OR ATMMACHINE?
S6        1096     LEGAL?()DOCUMENT? OR CAR()TITLE? OR MORTGAGE? OR WILL(2W)T-
                   ESTAMENT? OR DEED? ?

S7       2679565   ELECTRONIC? OR DIGITAL? OR PAPERLESS? OR PAPER()LESS? OR N-
                   ONPAPER OR NON()PAPER OR VIRTUAL?
S8        7194     (ASYNCHRON? OR ASYNCRON?)()TRANSFER?
S9        1741     PRIVATE?()(KEY OR KEYS OR KEYPAIR?)
S10       4601     (DECRYPT? OR PASSWORD? OR DECIPHER? OR ENCRYPT? OR ENCIPHE-
                   R?)()(KEY OR KEYS OR KEYPAIR?)
S11         0      ASSYM?(2N)CRYPT?
S12       1891     DIGITAL?()SIGNATUR?
S13       1957     (ELECTRONIC? OR ENCRYPT? OR ENCIPHER? OR HASH?)(3N)SIGNATU-
                   R?
S14      393925    IC=H04L?
S15      1302877   MC=(T01? OR W01?)
S16        407     S2(5N)S1 AND S3:S5
S17        405     S16 NOT S8
S18          1     S17 AND S6(7N)S7
S19          8     S17 AND S9:S13
S20          0     S18 AND S19
S21       39671    S3:S5 NOT S8
S22          6     S21 AND S7 AND (SAFEDEPOSIT? OR SAFETYDEPOSIT? OR (SAFE OR
                   SAFETY)()DEPOSIT?)
S23          1     S22 AND S9:S13
S24        267     S17 AND S14:S15
S25          2     S24 AND S9:S10 AND S12:S13
S26         13     S18:S19 OR S22:S23 OR S25
S27         13     IDPAT (sorted in duplicate/non-duplicate order).
File 347:JAPIO Nov 1976-2005/Apr(Updated 050801)
         (c) 2005 JPO & JAPIO
File 350:Derwent WPIX 1963-2005/UD,UM &UP=200555
         (c) 2005  Thomson Derwent
?
```

Pat Lit

Bibliog.

Files

evier.com

27/3,K/10   (Item 10 from file: 350)
DIALOG(R)File 350:Derwent WPIX
(c) 2005 Thomson Derwent. All rts. reserv.

013576265   **Image available**
WPI Acc No: 2001-060472/200107
Related WPI Acc No: 2002-672921; 2003-512941
XRPX Acc No: N01-045270
   Electronic **commerce and banking system for credit card payment system,**
  includes web bank in which access parameters are customized by web bank
  owner to control degree of access provided to third party
Patent Assignee: COHEN M E (COHE-I)
Inventor: COHEN M E
Number of Countries: 090 Number of Patents: 002
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
WO 200055793	A1	20000921	WO 2000US7457	A	20000320	200107	B
AU 200037659	A	20001004	AU 200037659	A	20000320	200107	

Priority Applications (No Type Date): US 99165231 P 19991111; US 99125008 P
  19990318; US 99280483 A 19990330; US 99130599 P 19990422; US 99130600 P
  19990422; US 99138428 P 19990610; US 99139167 P 19990615; US 99369902 A
  19990806; US 99161283 P 19991025
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 200055793	A1	E	103	G06F-017/60	

    Designated States (National): AE AL AM AT AU AZ BA BB BG BR BY CA CH CN
    CR CU CZ DE DK DM EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP
    KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX NO NZ PL PT RO RU SD SE
    SG SI SK SL TJ TM TR TT TZ UA UG US UZ VN YU ZA ZW
    Designated States (Regional): AT BE CH CY DE DK EA ES FI FR GB GH GM GR
    IE IT KE LS LU MC MW NL OA PT SD SE SL SZ TZ UG ZW
AU 200037659 A   Based on patent WO 200055793

    Electronic **commerce and banking system for credit card payment system,**
  includes web bank in which access...

Abstract (Basic):
...   For credit card payment system over internet such as **automatic**
  teller machine (**ATM**) wire transfers, programmable card transfer...

...site is simply and quickly established in cyber space where all bills to
  owner or **electronically** forwarded and archived. Enables owner to
  maintain **electronic safety deposit** boxes i.e. secure **electronic**
  sites where records are authenticated, time and date stamped and stored
  by metabank, thus improving...
Title Terms: **ELECTRONIC ;**

(51) International Patent Classification [7] : G06F 17/60	A1	(11) International Publication Number: WO 00/55793
		(43) International Publication Date: 21 September 2000 (21.09.00)

(54) Title: SYSTEMS FOR FINANCIAL AND ELECTRONIC COMMERCE

(57) Abstract

A system for electronic commerce including banking tools, products and services. The system includes customizable banking products (figure 7) and cards (figure 6), and methods and systems for conducting financial transactions (figure 9) and maintaining records over the Internet.

Server for storing and transmitting data

↓

Creation of a webbank by a user on server
(preferably via the Internet using a browser),
the server preferably being a central site
for all webbanks and being managed by
a central authority (such as a chartered bank),
with all transfers of information to or from
the server preferably being encrypted

↓

Transmissions of information to and from the user's webbank,
the transmissions being conducted by the user, by third parties,
and/or by the central authority, such as: transmissions
transferring funds between the webbank and any other financial
source (e.g. another webbank, a traditional bank or other
financial institution, a credit card, wire transfer or cash payment
to the central authority, etc.) and transmissions regulating,
managing or programming the accounts, subaccounts,
funds or other assets, and so forth, on the webbank

payment to the vendor's webbank, with the payment clearing instantaneously into that webbank. Thus, all steps in the invoicing process can be conducted in a matter of minutes. Likewise, all steps from the consumer's payment to clearance of payment can likewise be conducted in a matter of minutes using the webbank system once the consumer is ready to pay. Once payment is received, an electronic receipt can be forwarded back as well. If the vendor and consumer both wish, the entire cycle from invoicing to clearance of payment can be nearly instantaneous.

G. The Electronic Safety Deposit Box

The electronic safety deposit box is an online electronic lockbox associated with the webbank for storage, access, and recordkeeping of a user's important documents and assets. Accordingly, the user can easily and quickly access and present verified, digital copies of important documents and records from a central location, for self-access or presentation to third parties. Such documents can take advantage of date stamping, authentication, and other services provided by the metabank for providing security and trusted storage in online and traditional commercial transactions.

II. General Webbank Operation

A. Creation of Webbank

In accordance with the inventions disclosed herein, any entity with access to the Internet can open up its own private miniature bank located on the Internet, such private "webbank" being referred to herein as a webbank, webbank™, minibank or so forth. In the preferred embodiment, the entity opens up its webbank by logging into the overseer bank's website (also referred to herein as the metabank™ website) over a secure connection, so that the entity can open up its own website at the bank. Such website acts as the entity's webbank. The operation and creation of websites is well known in the art and all such hardware and software as are used for the operation and creation of such websites can be utilized in accordance with the present invention. The entity opening the webbank, is referred to herein as the "webbank owner".

In a preferred embodiment, the entity logs into the metabank's website, and fills out a form thereon over a secure connection. Once the form has been filled out, a website is created on the web, which is stored on the Company's server, in the same manner as is known in the art, and the webaddress for this website is provided to the webbank owner. This webaddress can (as with the other webaddresses disclosed herein) be any suitably long and random series of digits and/or letters desired. In accordance with the invention, the website serves as the control panel for the

12

are transferred between websites, or so forth, as disclosed in the present inventor's related applications listed above. In alternative embodiments, payments can also authorized by any other means, e.g. by telephone authorization by the user, and sent by any other means, including means well known in the art.

Preferably, in accordance with the invention, authenticated records are likewise transferred instantaneously at the same time as the financial transaction, immediately providing each webbank with an authenticated receipt documenting, verifying, confirming, and recording the transaction for future reference.

All transfers or payments made from the website are preferably made sufficiently secure methods, such as using encryption technology as is known in the art, or as further developed in the future. Assymetric or symmetric encryption can be used for sending information over the Internet, or a combination of both. Such encryption methods, including such methods as DES, Triple DES, RSA, PGP, among others, are known in the art, and are used to ensure high levels of security.

In a preferred embodiment, the systems used employ identification (e.g. by using digital certificates), authentication (e.g. by using digital signatures), nonrepudiation, verification and privacy. In one embodiment of the invention, the systems used make use of the processor serial number of the user's computer, for further security purposes.

In further alternative and/or additional embodiments of the invention, information and documents are also sent to the webbank to enable centralized storage of important records for access at any time by the user. Examples of the types of information which can be sent to the personal financial website include: receipts for purchases or payments, credit card statements, bills, tax return documents, real estate deeds, and any other desired information. This information is sent to the website (e.g. in the same manner that email is currently sent, and/or by sending in documents to a central authority which are scanned, and/or by providing electronic filings, authentications and certificates of such transactions, etc.) and is stored on the webbank, or in an appropriate linked area (e.g. on the overseer bank's server or on the server of an appropriate authority,whether private or governmental). Accordingly, when the user wants to access his or her credit card receipts, tax records, real estate deeds, marriage license, or so forth, he or she can dial up his or her personal financial website and access the relevant information thereon. In a further embodiment, a call is made by the user to the website, but the website dials back the user at a predetermined Internet address or phone number or other location (or emails the information to the user's preset email address) to reduce or obviate the possibility of breaches of security.

015563664   **Image available**
WPI Acc No: 2003-625820/200359
Related WPI Acc No: 2002-291315; 2002-350889; 2002-361074; 2002-403634;
   2002-434492; 2002-689576; 2003-016730; 2003-110525; 2003-597452;
   2003-606493; 2003-606496; 2003-606498; 2003-606499; 2003-606675;
   2003-616284; 2003-616533; 2003-659967; 2003-660122; 2003-661790;
   2003-661791; 2003-661792; 2003-662347; 2003-662348; 2003-811610;
   2004-120827; 2004-542520; 2005-110755; 2005-110756; 2005-110758;
   2005-110759; 2005-240070
XRPX Acc No: N03-497937
   **Central key authority database management method in account -based
   digital signature system for financial institution, involves
   maintaining record of information related to accounts, associated with
   public keys**
Patent Assignee: FIRST DATA CORP (FIRS-N)
Inventor: WHEELER A M; WHEELER L H
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
US 20030097573	A1	20030522	US 2000223076	P	20000804	200359	B
			WO 2001US41587	A	20010806		
			US 2003248622	A	20030201		

Priority Applications (No Type Date): US 2000223076 P 20000804; WO
   2001US41587 A 20010806; US 2003248622 A 20030201
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 20030097573	A1		128	H04L-009/00	Provisional application US 2000223076

                          Cont of application WO 2001US41587
   **Central key authority database management method in account -based
   digital signature system for financial institution, involves
   maintaining record of information related to accounts, associated with
   public keys**

Abstract (Basic):
...   of an account holder (202), is associated with the public key
   (218) of the public- **private** key pair of that account holder. A
   record of information belonging to the accounts of the...
...   For managing central key authority (CKA) database in
   account-based **digital   signature** (ABDS) system for managing
   financial institution **account** using integrated circuit (IC) card,
   credit card or **automated   teller** machine (**ATM**) card used in **ATM**
   machine, for managing brokerage account using personal digital
   assistant (PDA), bill payment services **account** using cell phone,
   credit bureau **account** , patient/personal medical records account,
   medical practice management account, government benefits account,
   Internet service provider, employee database authorization account,
   secure area authorization **account** in buildings and **electronic** data
   interchange with multiple purchasing agents. Also for use in e-business
   transactions, digital gift...

...The central key authority database including account information is
   effectively managed and the **accounts** are securely transferred over
   electronic communication system, with **accounts** being digitally
   signed...

...The figure shows the block diagram of account-based **digital   signature**
     system...
International Patent Class (Main): **H04L-009/00**
...Manual Codes (EPI/S-X): **T01-D01** ...

... **T01-J05A2** ...

... **T01-J05B4M** ...

... **T01-N01A1** ...

... **W01-A05**

(19) **United States**

(12) **Patent Application Publication** (10) Pub. No.: US 2003/0097573 A1
WHEELER et al. (43) Pub. Date: May 22, 2003

(54) **CENTRAL KEY AUTHORITY DATABASE IN AN ABDS SYSTEM**

(75) Inventors: **Lynn Henry WHEELER**, Greenwood Village, Colorado (US); **Anne M. Wheeler**, Greenwood Village, Colorado (US)

(73) Assignee: **First Data Corporation**, Suite 330K, Greenwood Village, 80111 Colorado (US)

(21) Appl. No.: **10/248,622**

(22) Filed: **Feb. 1, 2003**

Related U.S. Application Data

(63) Continuation of application No. PCT/US01/41587, filed on Aug. 6, 2001.

(60) Provisional application No. 60/223,076, filed on Aug. 4, 2000, now abandoned.

Publication Classification

(51) Int. Cl.^{7} **H04L 9/00**
(52) U.S. Cl. **713/182**

(57) **ABSTRACT**

Managing a database of a central key authority for a plurality of account holders, each account holder having at least one account associated with a public key of a public-private key pair of that account holder, includes maintaining for each account holder a record of information pertaining to the accounts of that account holder associated with the public keys of the account holder. The information pertaining to the accounts of an account holder includes (a) a public key of a user device that generates digital signatures, and (b) third-party account identifiers each of which identifies to a third-party an account of the user that is maintained with the third-party and that has been associated with the user's public key by the third-party.
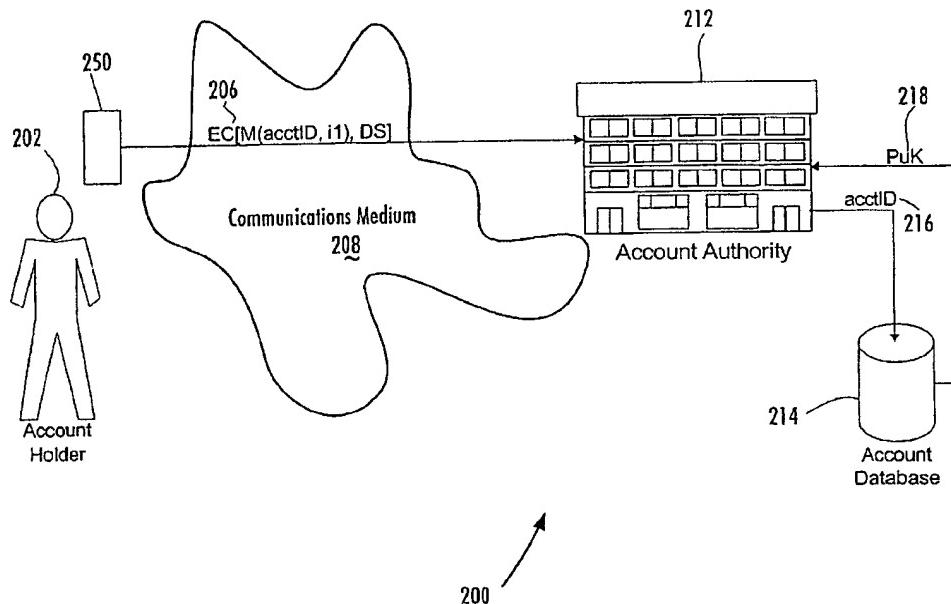
014434904   **Image available**
WPI Acc No: 2002-255607/200230
XRPX Acc No: N02-197650
   Optical disk e.g. CD, DVD for authenticating transactions over Internet,
   stores encrypted digital   signature **of user for signing financial**
   transactions over Internet
Patent Assignee: CK GLOBAL INC (CKGL-N); AARONS M T (AARO-I)
Inventor: AARONS M T
Number of Countries: 096 Number of Patents: 003
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
US 20020019938	A1	20020214	US 2000223204	P	20000804	200230	B
			US 2001921733	A	20010803		
WO 200212983	A2	20020214	WO 2001US41573	A	20010806	200230	
AU 200185402	A	20020218	AU 200185402	A	20010806	200244	

Priority Applications (No Type Date): US 2000223204 P 20000804; US
   2001921733 A 20010803
Patent Details:

Patent No	Kind Lan	Pg	Main IPC	Filing Notes
US 20020019938	A1	18	H04L-009/00	Provisional application US 2000223204

WO 200212983 A2 E   G06F-000/00
   Designated States (National): AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA
   CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN
   IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ
   PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG US UZ VN YU ZA ZW
   Designated States (Regional): AT BE CH CY DE DK EA ES FI FR GB GH GM GR
   IE IT KE LS LU MC MW MZ NL OA PT SD SE SL SZ TR TZ UG ZW
AU 200185402 A   H04L-009/00   Based on patent WO 200212983

Abstract (Basic):
...   The **digital   signature** is **encrypted** using password and
   stored in the disk for signing financial transactions over Internet.
...   Uses miniature CD, DVD for storing **digital   signatures** of
   user for cashing payroll, pay checks, identification of user for
   certified electronic mail concepts, income tax transactions and
   printing refund checks and for transferring refund money to **account**
   over Internet using **credit** card, **ATM** card and driver's license,
   also for authenticating access of personal computer...

...The figure shows a flowchart for storing user data, **digital   signature**
   and password...

(54) **METHOD AND APPARATUS FOR SECURE IDENTIFICATION FOR NETWORKED ENVIRONMENTS**

(76) Inventor: **Michael Thomas Aarons**, Fountain Valley, CA (US)

Correspondence Address:
KNOBBE MARTENS OLSON & BEAR LLP
620 NEWPORT CENTER DRIVE
SIXTEENTH FLOOR
NEWPORT BEACH, CA 92660 (US)

(57) **ABSTRACT**

Described is an apparatus for containment of Digital Personal Identity Signatures for use in completing and signing documents in a network or Internet environment. The apparatus contains a digital signature certificate issued by a third party that is used in place of an actual signature to allow completion of binding contracts through the use of a computer used over an Internet or Intranet environment. The apparatus includes a custom designed Compact Disc containing encrypted data and software that is used to access the digital signature in a secure environment. Access to the data is provided in a secure environment by requiring the use of an access password or Personal Identification Number, an alphabetic pass phrase or, an alphanumeric pass phrase to prevent fraudulent use of the digital signature in the event of loss or theft of the apparatus.

START

CAPTURE PHOTO—GRAPH OF REQUESTER

CAPTURE THUMB-PRINT OF REQUESTER

CAPTURE CURSIVE SIGNATURE OF REQUESTER

REQUEST MULTIPLE SIGNATURES FROM CA VIA ONLINE — TO CA

RECEIVE SIGNATURES FROM CA VIA ONLINE — FROM CA

REQUEST PASS PHRASE FROM USER

ENCRRYPT PHOTO THUMBPRINT, CURSIVE SIGNATURE AND EACH CA WITH MULTIPLE PASS PHRASES AS KEY

RECORD DATA ON MEDIA MULTIPLE TIMES

OPTIONALLY PRINT LABEL FOR FRONT OF MEDIA

PROVIDE USER WITH MEDIA

PREPARE DOCUMENT FOR SIGNING

REQUEST USER INSERT MEDIA IN CD OR DVD

REQUEST PASS PHRASE FROM USER

USE PASS PHRASE TO DECRYPT DATA

IS DECRYPTION OK? — NO

YES

ACCESS DATA FOR SIGNATURE

WRAP DOCUMENT WITH SIGNATURE

ATTACH PUBLIC KEY TO DOCUMENT

VERIFY IDENTITY OF PROCESSOR

SEND DOCUMENT TO PROCESSOR

(PREFERRED EMBODIMENT)

THIS APPLICATION
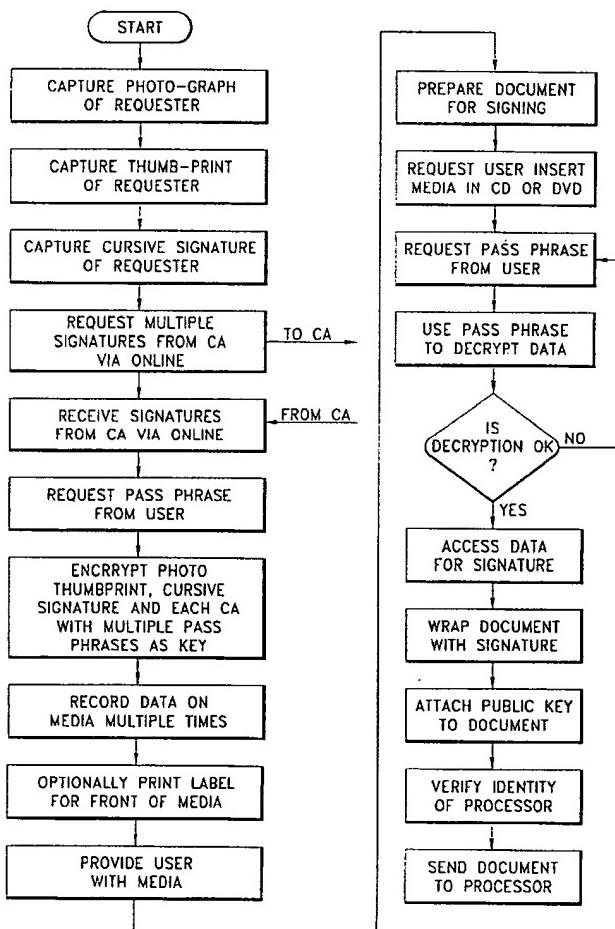
015059170   **Image available**
WPI Acc No: 2003-119686/200311
Related WPI Acc No: 2003-102262; 2003-119684
XRPX Acc No: N03-095339
     Digital   signature **apparatus for** automated   teller   **machine, has**
    computer processor which produces digital   signature **for** electronic
    document based on private   key **associated with** digital   safe
    deposit   account   **in disk drive**
Patent Assignee: DIEBOLD INC (DIEB-N)
Inventor: PARMELEE C L; SMITH M D
Number of Countries: 001   Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
US 20020129256	A1	20020912	US 2001273996	P	20010307	200311	B
			US 2001319015	P	20011129		
			US 2002683943	A	20020305		

Priority Applications (No Type Date): US 2002683943 A 20020305; US
    2001273996 P 20010307; US 2001319015 P 20011129
Patent Details:

Patent No	Kind Lan	Pg	Main IPC	Filing Notes
US 20020129256	A1	36	H04L-009/00	Provisional application US 2001273996

                                  Provisional application US 2001319015
     Digital   signature **apparatus for** automated   teller   **machine, has**
    computer processor which produces digital   signature **for** electronic
    document based on private   key **associated with** digital   safe
    deposit   account   **in disk drive**

Abstract (Basic):
...   A compact disk drive (26) stores several **digital safe**
    deposit accounts (40) associated with a **private key** (44). A
    computer processor in communication with the automated transaction
    machines (**ATMs**), produces a **digital signature** for an **electronic**
    document (42) based on the **private key** .
...   An INDEPENDENT CLAIM is included for **digital signature**
    method...

...For **digitally** signing **electronic** documents for **automated teller**
    machine...

...Enables to be easily employed by individuals for protecting and
    digitally signing the **electronic** documents. Preserves the integrity
    and confidentiality of the **electronic** documents for long time periods
    ...

...The figure shows a schematic view of the **digital signature** system...

... **Digital safe deposit accounts** (40...

... **Electronic** documents (42...

... **Private key** (44
Title Terms: **DIGITAL** ;
International Patent Class (Main): **H04L-009/00**
Manual Codes (EPI/S-X): **T01-D01** ...

... T01-N02B1 ...

... W01-A05A

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L2	13125	(automatic or automated) adj teller	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT	OR	ON	2005/08/30 13:10
L3	11761	private adj (key or keys)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT	OR	ON	2005/08/30 13:10
L4	12150	digital adj signature	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT	OR	ON	2005/08/30 13:10
L5	28250	account near3 (financial bank savings checking deposit electronic debit credit)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT	OR	ON	2005/08/30 13:11
L6	116183	(atm atms) not asynchron$ adj (transfer transferral transferring)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT	OR	ON	2005/08/30 13:12
L7	458	(2 6) and 3 and 4 and 5	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT	OR	ON	2005/08/30 13:12
L8	230	7 and @ad<"20010308"	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT	OR		30 13:44
L15	533	(safe adj deposit) adj (box boxes)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT	OR		30 13:16
L16	9	safedeposit adj (box boxes)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT	OR		www.els 30 13:16
L17	533	15 16 and 8	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT	OR	ON	2005/08/30 13:16

L21	44	electronic with (15 16)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT	OR	ON	2005/08/30 13:48

(19) **United States**

(12) **Patent Application Publication** (10) Pub. No.: US 2004/0024714 A1
Wells et al. (43) Pub. Date: Feb. 5, 2004

(54) **ELECTRONIC SAFE DEPOSIT BOX**

(76) Inventors: **Thomas E. Wells**, Coral Gables, FL
(US); **Eric K. Yee**, Fremont, CA (US)

Correspondence Address:
GARDNER CARTON & DOUGLAS LLP
191 N. WACKER DRIVE, SUITE 3700
CHICAGO, IL 60606 (US)

(21) Appl. No.: **10/168,944**

(22) PCT Filed: **Dec. 29, 2000**

(86) PCT No.: **PCT/US00/35552**

Related U.S. Application Data

(60) Provisional application No. 60/174,053, filed on Dec. 30, 1999.

Publication Classification

(51) Int. Cl.⁷ G06F 17/60

(52) U.S. Cl. 705/78

(57) **ABSTRACT**

An electronic safe deposit box system (the "ESDB System") is disclosed. The ESDB System identifies each of the users and each of the electronic files representing written information, data or documents with an alphanumeric code. The ESDB System electronically stores written information, data and documents sent to the ESDB System. Electronic maintained in the ESDB System may be accessed using an open network or group of servers such as the Internet or a closed network or group of servers such as an Intranet or LAN. Each user has a user identification, password and personal identification number ("PIN"). The ESDB System allows the user to designate third parties to access a user-controlled electronic safe deposit box. The third party may only view or print specific electronic files to which the user has previously granted the third party access. In addition, the ESDB System tracks the activity of third parties within the user's electronic safe deposit box, and automatically notifies, by email, the owner of the box of such activities.

FREELEGALONLINE
Providing information to address your legal needs

Bankruptcy and Collections LEGAL DEPARTMENT | Estate Planning LEGAL DEPARTMENT | Real Estate LEGAL DEPARTMENT | Start-Up and Small Business LEGAL DEPARTMENT

Search: [ ] [GO!]

|Become a Member
|STOREDOCSONLINE
|FREELEGALONLINE Store
|Our Partners

|Lawyers and Law Firms
|Legal Glossary
|Chat Room
|Feedback

|About FREELEGALONLINE
|Legal Services Statement
|Privacy & Security

Recent News

● FREELEGALONLINE signs strategic partnership with Microsoft
● Law requiring pre-abortion notice by doctors to parents blocked by Florida court
● Class action lawsuit alleges banks and credit card companies illegally collection Internet gambling debts

Upcoming Chat

● Weekly Chat Room Celeb Roy Black, Esq. talk with Mr. Black on Friday night, October 8, 1999, from 8 p.m. to 10 p.m.

MEMBERSHIP BENEFITS

Free monthly electronic newsletter

Notice of our chat room and online seminar topics

Notice of magazine and newspaper articles that affect you

Access to your online safe deposit box and our archived seminars

Valuable membership discounts
◇
CLICK HERE TO REGISTER

INTERNETWORKING POWER BY BEN

Office DEPOT

Fleet
Ready When You Are

amazon.com

Help • Customer Service • Site Index • Jobs • Advertising

[0038] If the user requested to add/delete/modify third party access by clicking on the hypertext link 60 in FIG. 4, the ESDB System presents the user with a dynamic HTML page as shown in FIG. 10. This page shows the third parties who have access to certain folders or files in the user's electronic safe deposit box as shown in box 61. The user would click on to a hypertext link of a specific name in box 61 if he wanted to delete or modify the access of any such third party. The user also has the option of granting a new party access to certain folders or electronic files in his box by inserting the new third party's member log-in/user identification in box 62. If the requested third party is not a member, the user can send an automatic email to such third party resting that such party become a member of the ESDB System by inserting the email address of the third party in box 63 and pressing the "Submit/Send" key in box 64. The user also has an option of adding an additional personalized comment to the automatic email by inserting text into box 65 before pressing the "Submit/Send" key shown in box 64. The user can obtain assistance by pressing the "Help" key in box 66 that would then send the user to an electronic help desk with answers to frequently asked questions as well as the ability to send an email question to the administrator of the ESDB System.

[0039] If the user clicked "JohnEsq" shown as a hypertext link 67 in FIG. 10 and pressed the "Submit/Send" key in box 64, the ESDB System presents the user with a dynamic HTML page shown in FIG. 11. This page allows the user to delete the access of "JobnEsq" to the folders and electronic files to which he currently has access by using the options in menu 70. Such access is deleted by clicking the hypertext link folder (which would delete the access of "JohnEsq" to all of the documents in that folder) as shown in hypertext link box 71 or by clicking the specific hypertext link electronic file shown in links 72 and 73 and then pressing the "Delete Access" key shown in box 74. The user can obtain assistance by pressing the "Help" key in box 75 that would then send the user to an electronic help desk with answers to frequently asked questions as well as the ability to send an email question to the administrator of the ESDB System.

[0040] The user can grant "JohnEsq" greater access to folders or specific electronic files contained in the user's electronic safe deposit box by selecting one of the hypertext links in box 76 shown in FIG. 11. Box 76 displays all of the folders and the electronic files in each folder to which "JohnEsq" does not currently have access. The user can grant "JohnEsq" access to all of the electronic files contained in a folder by clicking one or more hypertext link folders shown in links 77, 78, 79, 80, and 81 or access to a specific electronic file by clicking one or more of the hypertext link files shown in links 82, 83, 84, 85, 86, 87, 88, 89 and 90. After the user makes his selection, he presses the "Grant Access" key shown in box 91 which allows the ESDB System to record the requested action and grant "JohnEsq" access to the selected folder(s) or electric file(s). The user can obtain assistance by pressing the "Help" key in box 92 that would then send the user to an electronic help desk with answers to frequently asked questions as well as the ability to send an email question to the administrator of the ESDB System.

[0041] The ESDB System records the activity in a user's electronic safe deposit box and can display such activity by the user clicking the "Click here to review prior box activ-

ity" hypertext link 100 in FIG. 4. When such link is pressed, the user is shown a dynamic HTML page similar to FIG. 12. The information in box 101 indicates the prior activity for the user's electronic safe deposit box for the last 3 months as referenced in item 102. The ESDB System can display the activity in the user's box for any period of time (including periods exceeding 3 months) depending upon the programmable parameters of the ESDB System. The user can return to me previous page by pressing the "Back to Prior Screen" link 103.

[0042] While the invention has been described in the context of a preferred embodiment, it will be apparent to those skilled in the art that the present invention may be modified in numerous ways and may assume many embodiments other than that specifically set out and described above. Accordingly, it is intended by the appended claims to cover all modifications of the invention that fall within the true scope of the invention.

[0043] Benefits, other advantages, and solutions to problems have been described above with regard to specific embodiments. However, the benefits, advantages, solutions to problems, and any element(s) that may cause any benefit, advantage, or solution to occur or become more pronounced are not to be construed as a critical, required, or essential feature or element of any or all the claims. As used herein, the terms "comprises,""comprising," or any other variation thereof, are intended to cover a non-exclusive inclusion, such that a process, method, article, or apparatus that comprises a list of elements does not include only those elements but may include other elements not expressly listed or inherent to such process, method, article, or apparatus.

What is claimed is:

1. A computerized system for managing electronic data of a user over a network of computers comprising:

an electronic safe deposit box in electrical communication with said user, wherein said electronic safe deposit box stores a first user data file and a second user data file;

an alphanumeric designator which designates a first alphanumeric code to said fist data file and a second alphanumeric code to said second data file; and

an access controller to manage access to said electronic safe deposit box, said access controller interfacing via said network of computers with a third party having a unique designator.

2. The computerized system for managing electronic data of claim 1, wherein said user can designate a set of access privileges for said third party, said access privileges stored.

3. The computerized system for managing electronic data of claim 2, wherein said access privileges comprise read privileges.

4. The computerized system for managing electronic data of claim 3, wherein said access privileges comprise print privileges.

5. The computerized system for managing electronic data of claim 4, wherein said access privileges comprise modify privileges.

6. The computerized system for managing electronic data of claim 2, wherein said access controller prompts said third party to enter said unique designator, and determines whether said third party is authorized to access said electronic safe deposit box.

7. The computerized system for managing electronic data of claim 6, wherein said access controller prompts said third party to enter said first alphanumeric code to access said first data file.

8. The computerized system for managing electronic data of claim 7, wherein said access controller prompts said third party to enter said second alphanumeric code to access said second data file.

9. The computerized system for managing electronic data of claim 8, wherein said access controller monitors access to said electronic safe deposit box by said third party.

10. The computerized system for managing electronic data of claim 9, wherein said access controller automatically notifies said user when said third party commences access to said electronic safe deposit box.

11. The computerized system for managing electronic data of claim 9, wherein said access controller automatically notifies said user when said third party terminates access to said electronic safe deposit box.

12. The computerized system for managing electronic data of claim 9, wherein said access controller automatically notifies said user of a set of activities performed by said third party in relation to said first user data file.

* * * * *

(51) International Patent Classification[7]: G06F 17/30

(21) International Application Number: PCT/US01/06419

(22) International Filing Date: 28 February 2001 (28.02.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/514,726   28 February 2000 (28.02.2000)   US

(71) Applicant: **B4BPARTNER, INC.** [US/US]; Suite 201, 300 Sevilla Avenue, Coral Gables, FL 33134 (US).

(72) Inventors: **WELLS, Thomas, O.**; 1301 Sorolla Avenue, Coral Gables, FL 33134 (US). **YEE, Eric, K.**; 917 Tendilla Avenue, Coral Gables, FL 33134 (US).

(74) Agent: **DINOVO, Andrew, G.**; Vinson & Elkins L.L.P., 2300 First City Tower, 1001 Fannin, Houston, TX 77002-6760 (US).

(81) Designated States (national): AU, CA, CN, JP, MX, RU.

(84) Designated States (regional): European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

Published:
— without international search report and to be republished upon receipt of that report

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: COMPUTERIZED COMMUNICATION PLATFORM FOR ELECTRONIC DOCUMENTS

(57) **Abstract:** An integrated electronic document management system and method is disclosed for generating, storing, retrieving, handling, tracking, transmitting, encrypting, decrypting and using electronic documents in a network or online environment. When generating a document, a template and question and answer file are communicated to the user's browser corresponding to a user-selected document type. Answers to the questions are input directly into the document-in-progress as they are entered by the user. An answer file is then sent to a server to generate the electronic document. The electronic document may be securely stored in an electronic safe deposit box. Activity with an electronic safe deposit box is tracked, and automatic email notices are periodically sent to users of the computer network. The network further facilitates the issuance of a private and public key to users associated with a unique alphanumeric pass-phrase allowing the user to encrypt, decrypt and digitally sign electronic documents within the computer network.

**COMPUTERIZED COMMUNICATION PLATFORM
FOR ELECTRONIC DOCUMENTS**

COPYRIGHT NOTICE

5   A portion of the disclosure of this patent document contains material which is subject

to copyright protection. The protection owner has no objection to the facsimile reproduction

by anyone of the patent document, or of the patent disclosure as it appears in the Patent and

Trademark Office patent files or records, but otherwise reserves all copyrights whatsoever.

10 **I.   FIELD OF THE INVENTION**

        The invention relates to the generation, storage, retrieval, handling, tracking,

distribution, encrypting, decrypting and use of electronic documents, and more particularly to

efficient and secure storage, retrieval, access and use of electronic documents on an open

network or group of servers such as the Internet, a closed network or group of servers such as

15 an Intranet, or a local area network ("LAN"), and recording and reporting the access to and

the activities performed with respect to such electronically-stored information, data and

documents.

II.   BACKGROUND OF THE INVENTION

20   The generation of electronic documents has long been accomplished by word

processor applications and other programs such as computer aided-design ("CAD")

applications, databases and spreadsheets. An obvious advantage of electronic documents is

that they are often similar to, or based upon, earlier documents, and the earlier documents can

simply be modified to generate the new document.

25   A common problem with the generation of electronic documents via this modification

method, however, is that the user must manually search for the location of information that

must be replaced, and manually replace it. Oftentimes, certain items of old information are

Fig. 21 that allows the user to move a copy of an electronic document from the user's personal computer or server to the Inbox Contents of his electronic safe deposit box.

The user has the option of placing a copy of an electronic document from the Save Deposit Box Contents to the Document Viewing Room. When the user moves the document to the Document Viewing Room, the ESDB System will automatically generate an alphanumeric pass-phrase for such electronic document and prompt the user to provide an email address to send the pass-phrase to the recipient. When the email is transmitted, the recipient will receive the email with the pass-phrase and a hypertext link to the ESDB System. When the recipient depresses the hypertext link, the recipient will be presented with a screen welcoming him to the ESDB System. If the recipient's email address and pass-phrase correspond with the information contained in the ESDB System's database with respect to such electronic document, the recipient will be able to view the electronic document. The recipient will not be able to download or modify the electronic document. Future versions of the ESDB System will provide for the email to be encrypted using a double-key process residing within the ESDB System.

The ESDB System will assign a private key and public key to each user (i.e., owner of an electronic safe deposit box). The user may use his public key to encrypt documents within his electronic safe deposit box. The double key system will reside within the ESDB System. The ESDB System will associate the user with his private key when the user provides a unique alphanumeric phrase assigned to the user within the ESDB System. By having the double key system reside within the ESDB System and accessible by providing a alphanumeric phrase, the user will may view his encrypted documents from any computer and the user may digitally sign documents through a "one-click" process in which the user clicks a "SIGN DOCUMENT" button and then provides his unique alphanumeric phrase associated with the user's private key. This process is much simpler than current applications and methods of private and public key systems.

CLAIMS

What is claimed is:

1.   A computerized system for managing electronic documents by a user over a network
5   of computers comprising:

an interactive document generator for generating an electronic document, the
document generator including a connection for a user terminal;

an electronic safe deposit box in electronic communication with said document
generator, wherein said electronic safe deposit box stores document
10   content data corresponding to said electronic document;

a document handler allowing said user to view and modify said electronic
document from said user terminal and track activity associated with a
user's electronic safe deposit box; and

a document transmitter with which said user can cause such electronic
15   document to be transmitted to a third party remote from said systems.

2.   The computerized system for managing electronic documents of claim 1, further
comprising a computer telefacsimile receiver that allows documents to be
faxed/encrypted directly into the user's Inbox Contents of his electronic safe deposit
20   box.

3.   The computerized system for managing electronic documents of claim 2, further
comprising a computer email sender which automatically notifies the user of box
activity on a periodic basis and allows the user to email electronic documents from his
25   Save Deposit Box Contents.

4.   The computerized system for managing electronic documents of claim 3, further
comprising:

a private and public key computer generator which automatically assigns
30   private and public keys to users for encryption, decryption and digital
signatures of electronic documents associated with a unique
alphanumeric pass-phrase; and

a cipher that enciphers and deciphers electronic documents.

35 5.   The computerized system of claim 4, wherein said document generator comprises a

- 20 -

private key and a public key to said user, said private key and public key both being associated with a unique alphanumeric pass-phrase, to allow the user to digitally sign electronic documents within the system.

5   24.   The computerized system of claim 4, further comprising a document sharing subsystem for said user to share said electronic document with a third party, said document sharing subsystem comprising an e-mail notification for notifying said third party, said e-mail notification being sent from said system and including a unique alphanumeric pass-phrase and a hypertext link back to
10   said system, whereby said third party can access said electronic document by submitting said pass-phrase to said system.

15

- 23 -

```
Set      Items    Description
S1     1381151    ACCOUNT?
S2     3608755    SAFEDEPOSIT? OR SAFE?()DEPOSIT? OR SAFETYDEPOSIT? OR ELECT-
                  RONIC? OR FINANCIAL? OR CHECKING? OR SAVINGS? OR DEBIT OR CRE-
                  DIT? OR BANK?
S3        3443    AUTOMAT?()TELLER?
S4           5    (DRIVE()UP OR DRIVE()THRU OR DRIVEUP OR DRIVETHRU)(2N)(BAN-
                  K? OR TELLER?)
S5      116071    ATM OR ATMS OR ATMMACHINE?
S6       58447    LEGAL?()DOCUMENT? OR CAR()TITLE? OR MORTGAGE? OR WILL(2W)T-
                  ESTAMENT? OR DEED? ?

S7     3673602    ELECTRONIC? OR DIGITAL? OR PAPERLESS? OR PAPER()LESS? OR N-
                  ONPAPER OR NON()PAPER OR VIRTUAL?
S8       37842    (ASYNCHRON? OR ASYNCRON?)()TRANSFER?
S9        1926    PRIVATE?()(KEY OR KEYS OR KEYPAIR?)
S10       1532    (DECRYPT? OR PASSWORD? OR DECIPHER? OR ENCRYPT? OR ENCIPHE-
                  R?)()(KEY OR KEYS OR KEYPAIR?)
S11       1000    (ASSYM? OR ASYM?)(2N)(CRYPT? OR ENCRYPT? OR ENCIPHER? OR D-
                  ECRYPT? OR DECIPHER?)
S12       8192    DIGITAL?()SIGNATUR?
S13       3261    (ELECTRONIC? OR ENCRYPT? OR ENCIPHER? OR HASH?)(3N)SIGNATU-
                  R?
S14        146    S1(5N)S2 AND S3:S5
S15          0    S14 AND S6 AND S7
S16        143    S14 NOT S8
S17          1    S16 AND S9:S13
S18      84801    S3:S5 NOT S8
S19          1    S18 AND S7 AND (SAFEDEPOSIT? OR SAFETYDEPOSIT? OR SAFE?()D-
                  EPOSIT?)
S20          2    S17 OR S19
S21          1    RD (unique items)
S22          3    S9 AND S12 AND S3:S5
S23          3    RD (unique items)
S24         47    S9:S13 AND S3:S5
S25         30    S24 NOT S8
S26         15    S25 AND S7(7N)(S1:S2 OR S6)
S27         12    RD (unique items)
S28         11    S27 NOT (S21 OR S23)
File    2:INSPEC 1969-2005/Aug W3
           (c) 2005 Institution of Electrical Engineers
File    6:NTIS 1964-2005/Aug W2
           (c) 2005 NTIS, Intl Cpyrght All Rights Res
File    8:Ei Compendex(R) 1970-2005/Aug W3
           (c) 2005 Elsevier Eng.  Info. Inc.
File   34:SciSearch(R) Cited Ref Sci 1990-2005/Aug W3
           (c) 2005 Inst for Sci Info
File   35:Dissertation Abs Online 1861-2005/Aug
           (c) 2005 ProQuest Info&Learning
File   65:Inside Conferences 1993-2005/Aug W4
           (c) 2005 BLDSC all rts. reserv.
File   94:JICST-EPlus 1985-2005/Jul W1
           (c)2005 Japan Science and Tech Corp(JST)
File   99:Wilson Appl. Sci & Tech Abs 1983-2005/Jul
           (c) 2005 The HW Wilson Co.
File  111:TGG Natl.Newspaper Index(SM) 1979-2005/Aug 29
           (c) 2005 The Gale Group
File  144:Pascal 1973-2005/Aug W3
           (c) 2005 INIST/CNRS
File  239:Mathsci 1940-2005/Oct
           (c) 2005 American Mathematical Society
```

Non Pat Lit

Bibliog Files

evier.com

23/3,K/1   **(Item 1 from file: 2)**
DIALOG(R)File   2:INSPEC
(c) 2005 Institution of Electrical Engineers. All rts. reserv.

6251270   INSPEC Abstract Number: B1999-06-6150M-090
   **Title: Certificate path generating protocol (CPGP) for authenticated
signaling in ATM networks**
   Author(s): Jun Xu; Singhal, M.
   Author Affiliation: Dept. of Comput. & Inf. Sci., Ohio State Univ.,
Columbus, OH, USA
   **Title: Certificate path generating protocol (CPGP) for authenticated
signaling in ATM networks**
   Abstract: Authenticated signaling is an important security service to be
provided by **ATM** networks to guard against threats of spoofing and
impersonation. The **ATM** Forum specifies public key cryptography to be the
default **ATM** authentication mechanism and directory services like X.509 to
be the infrastructure for public key...

... With public key cryptography, authenticated signaling requires the
signaling message to be authenticated with a **digital   signature** signed
by the **private   key** of the calling party. To verify the **digital
signature** , the called party needs to obtain the public key of the calling
party and a...

... called the certificate path between two parties. The certificate
exchange protocol (CEP), proposed by the **ATM** Forum, requires that another
bi-directional connection be established between two parties to change
public...

... an ideal approach. We propose a certificate path generating protocol
(CPGP), which is embedded into **ATM** signaling and routing protocols to
generate a certificate path inside a signaling message on-the-fly as the
signaling message travels through the **ATM** network. In CPGP all that a
calling party needs to do for authenticated signaling is to put into the
signaling message its own public key certificate and the **digital
signature** of the signaling message signed using its **private   key** . The
CPGP builds the rest of the certificate path for it. The proposed protocol
is embedded into the **ATM** signaling and routing protocol so that no
performance overhead is incurred to establish the certificate...
   ...Identifiers: **ATM** networks...

... **ATM** Forum...

... **digital   signature** ; ...

... **private   key** ; ...

... **ATM** signaling protocols

23/3,K/2   (Item 1 from file: 8)
DIALOG(R)File   8:Ei Compendex(R)
(c) 2005 Elsevier Eng. Info. Inc. All rts. reserv.

05161394   E.I. No: EIP98114467227
   Title: Certificate Path Generating Protocol (CPGP) for authenticated signaling in ATM networks
   Author: Xu, Jun; Singhal, Mukesh
   Corporate Source: Ohio State Univ, Columbus, OH, USA
   Conference Title: Proceedings of the 1998 International Conference on Network Protocols, ICNP
   Conference Location: Austin, TX, USA   Conference Date: 19981013-19981016
   E.I. Conference No.: 49210
   Source: International Conference on Network Protocols 1998. IEEE Comp Soc, Los Alamitos, CA, USA,98TB100256. p 282-289
   Publication Year: 1998
   CODEN: 85QDAI
   Language: English

   Title: Certificate Path Generating Protocol (CPGP) for authenticated signaling in ATM networks
   Abstract: Certificate path generating protocol (CPGP) is proposed for authenticated signaling, which is embedded into **ATM** signaling and routing protocols to generate a certificate path inside a signaling message on-the-fly as the signaling message travels through the **ATM** network. In CPGP, all that a calling party needs to do for authenticated signaling is to put into the signaling message its own public key certificate and the **digital   signature** of the signaling message signed using its **private key** . CPGP builds the rest of the certificate path for it. The proposed protocol is embedded into the **ATM** signaling and routing protocol so that no performance overhead is incurred to establish the certificate...

28/3,K/1   (Item 1 from file: 2)
DIALOG(R)File   2:INSPEC
(c) 2005 Institution of Electrical Engineers. All rts. reserv.

6825048
  Title: Merrill makes decision to streamline online forms management with Silanis software
  Author(s): Simms, M.
  Journal: Wall Street & Technology   vol.18, no.12   p.70
  Publisher: CMP Media Inc,
  Publication Date: Dec. 2000 Country of Publication: USA
  CODEN: WSTEE5 ISSN: 1060-989X
  SICI: 1060-989X(200012)18:12L.70:MMDS;1-1
  Material Identity Number: P708-2000-014
  Language: English
  Subfile: D
  Copyright 2001, IEE

  Abstract: Merrill Lynch signed on with Silanis Technology to test the company's **electronic   signature** software, a pilot that will initially be deployed internally and then in the brokerage firm...

  ... be available to users via the firm's Web site, helping Merrill streamline its online **electronic** document procedures. An online user creates what's called an ePersona, which contains personal information, including his or her handwritten signature. A **private   key** identifier is assigned to the ePersona so, similar to the PIN a customer memorizes to use his or her **ATM** card, the ePersona ID is unique to the user, adding a layer of security. The software permanently imbeds the **electronic signature** to an **electronic** form such that, should the document or the signature be altered in any way, the...
    ...Descriptors: **electronic** commerce
    ...Identifiers: **electronic   signature** software

28/3,K/6   (Item 2 from file: 8)
DIALOG(R)File   8:Ei Compendex(R)
(c) 2005 Elsevier Eng. Info. Inc. All rts. reserv.

01913515   E.I. Monthly No: EIM8512-079798
  Title: SMART CARDS, DIGITAL   SIGNATURES **AND NEGOTIABLE DOCUMENTS.**
  Author: Davies, D. W.
  Corporate Source: Natl Physical Lab, Teddington, Engl
  Conference   Title: International   Conference   on Secure Communication
Systems.
  Conference Location: London, Engl   Conference Date: 19840222
  E.I. Conference No.: 05466
  Source: IEE Conference Publication n 231. Publ by IEE, London, Engl p 1-4
  Publication Year: 1984
  CODEN: IECPB4   ISBN: 0-85296288-6
  Language: English

  Title: SMART CARDS, DIGITAL   SIGNATURES **AND NEGOTIABLE DOCUMENTS.**
  ...Abstract: these already exists in large numbers and is very successful
namely the cash dispenser or **automatic   teller** machine (**ATM**) with its
plastic, magnetic striped card and personal identification number.
Authentication of **digital   signatures** , **enciphering** and deciphering
functions, **electronic** checks, **signature** tokens for negotiable documents
and other types of secret keying as a protection against theft...
  Identifiers: PAYMENT SYSTEMS; **AUTOMATIC   TELLER** MACHINE; MAGNETIC
STRIPED CARDS; SIGNATURE VERIFICATION SCHEME; SMART CARDS

altavista Web   Images   MP3/Audio   Video   News   Family Filter: **off**   Help

Advanced Web Search

Search with...

this boolean
expression

```
"electronic safe deposit"
OR "electronic safety deposit"
```

FIND

Use terms such as AND, OR, NOT
More>>

SEARCH: ○ Worldwide ◉ USA   **RESULTS IN:** ◉ All languages ○ English, Spanish

AltaVista found 14 results

TechTalk: Your computer: An electronic safe deposit box (05-04-95)
UpDate - Vol. 14, No. 30, Page 10 May 4, 1995 TechTalk Your computer: An **electronic safe deposit** box The scenario: Jane answers her office phone one afternoon to find her neighbor, Claire, on the line.
www.udel.edu/PR/UpDate/95/30/22.html
More pages from udel.edu

Century Hong Kong Hotel situated in Wanchai.
Century Hong Kong hotel in Wanchai, Hong Kong, at the heart of the busiest city. Near the Wanchai MRT station and many entertainment establishments. ... Each room is complete with **electronic safe deposit** box, multi-function touch screen smart phone with voice mail system ...
www.orientaltravel.com/hotel/city1/det_centuryhk.htm
More pages from orientaltravel.com

Century HK
Hotel Information. Century Hong Kong Hotel. 238 Jaffe Road, Wanchai ... Each room is complete with **electronic safe deposit** box, multi-function touch screen smart phone with voice mail system ...
www.orientaltravel.com/hotel/city1/det_century.htm
More pages from orientaltravel.com
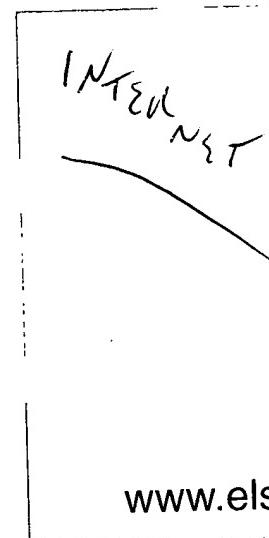
Traveler's Haven - Hotels & Tours by Area
... a/c, lavish bath, satellite color TV, telephone, mini bar, ceiling fans, hair dryer, **electronic safety deposit** box. ...
www.travelershaven.com/hotels_tours/n_pacific/h_meliaconchal.html
More pages from travelershaven.com

Bailemen Hotel Shanghai
... audio system, international direct dial phone, closed-circuit TV, refrigerator and **electronic safety deposit** box ...
ulink.ourfamily.com/hotelNet/hotels/shanghai/bl_ind.htm
More pages from ulink.ourfamily.com

eLAYOVER - NEWS STORY AND TIPS PAGE
... We look upon it as a kind of free **electronic safe-deposit** box where you can store just about anything ...
elayover.com/news-1.html
More pages from elayover.com

www.ellada.net/ads/details/hotelmo27.html

12 октября 2001 года

НОВОСТИ

Главные новости   Лента новостей
Рейтинг новостей   Словари Подписка

Автомобили / Бизнес / Здоровье / Кино / Компьютеры / Космос / Массмедиа / Мода / Музыка / Обзор прессы / Политика / Сплетни / Спорт / Туризм

Навигатор   Развлечения   Новости   Каталог   Общение   Рефераты   Личный каб.
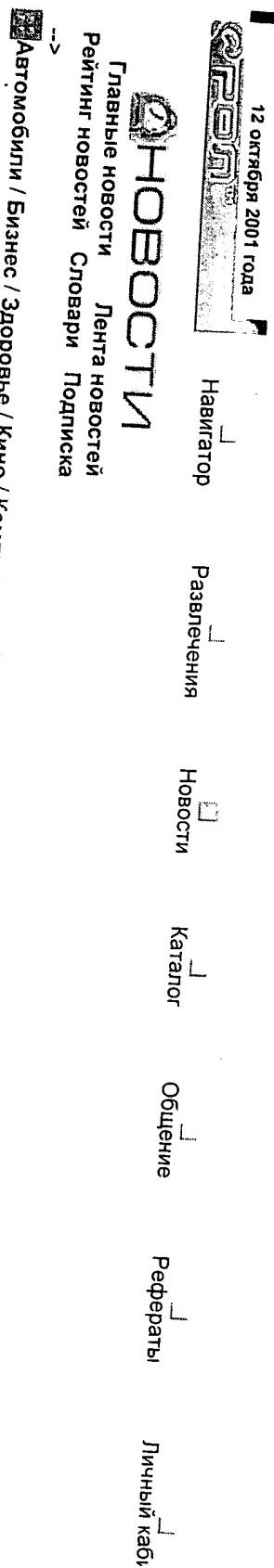
Fleet Introduces 'fileTRUST', Online Data 'Safe Deposit Box' and Wins Microsoft Innovation Award; First Bank in Nation to Develop Online Document Storage Tool

Business/Banking Editors

BOSTON--(BUSINESS WIRE)--Oct. 10, 2000--FleetBoston Financial today announced the pilot launch of fileTRUST(SM) online data storage (www.filetrust.com), the first-ever Web-based "safe deposit box" developed by a bank for its customers to securely store and access important electronic documents and images. A proprietary system, fileTRUST was created by Fleet in conjunction with Microsoft Consulting Storage and in partnership with EMC2, Compaq Computer Corporation, Plural, Inc., and StorageNetworks, Inc.

fileTRUST is initially aimed at the growing number of home offices and small business professionals such as lawyers, certified public accountants and doctors who typically do not own costly backup file servers but who need to ensure the safety and integrity of their files and records. Users may rent space at fileTRUST and, with a personal identification number and password, can easily upload or download their files via the Web 24 hours day. Document storage enables a business owner to expand memory capacity without having to upgrade hardware and guarantees that files will be protected from deadly viruses, computer damage or system failure.

Fleet plans to initially test fileTRUST with a select group of Fleet Small Business Services clients and eventually make it available to any individual or company in need of secure document storage. Larger companies will use fileTRUST to simplify internal processes and create efficient communications with their customers. Consumers also will be able to use fileTRUST directly to store their personal documents.

"This product reinforces Fleet's commitment to offering Web-based products to our customers that are safe, of the highest quality, and that provide added value. fileTRUST users can trust that their sensitive files and information are safe on the Web in their electronic safety deposit box," said Blaise Heltai, managing director, Global Internet Strategy at FleetBoston Financial. "The powerful technical architecture that fileTRUST was built upon offers 'best of class' security and convenience in online storage, and provides the additional capabilities of collaboration and document sharing. As users of fileTRUST ourselves, we offer a compelling case for the value of the service."

At its simplest, users can view fileTRUST as another disk drive in their Windows file viewer or as a Web location in their browser. Along with general document storage, fileTRUST allows users to designate guest access to view specific files in their secure area. In this way, fileTRUST serves as the cornerstone for other strategic applications such as document certification, project

management, and workflow-facilitation across businesses. "fileTRUST demonstrates the power and flexibility of Exchange 2000 as a platform for hosted application services," said Russ Stockdale, vice president of the Knowledge Worker Solutions Group at Microsoft. "FleetBoston is an early mover in developing software as a service and innovating on Microsoft's .NET platform."

Winner of the Microsoft Exchange and Collaboration (MEC) 2000 Solutions Award for Most Innovative Use of the Exchange 2000 Web Storage System, fileTRUST online data storage was produced as part of the e-Catalyst effort within Fleet, a corporate-wide initiative for creating top-tier Web-enabled services for customers and employees.

"Fleet is committed to developing solutions that help small business owners and entrepreneurs run their business," said Norman DeLuca, managing director, Small Business Services at FleetBoston Financial. "fileTRUST is ideal for our small business customers who need to store and share confidential documents with multiple users in a secure environment."

FleetBoston Financial is the eighth-largest financial holding company in the United States. A $181 billion diversified financial services company, it offers a comprehensive array of innovative financial solutions to 20 million customers in more than 20 countries and territories. Among the company's key lines of business are: retail banking, with over 1,250 branches and over 3,400 ATMs in the Northeast; commercial banking, including capital markets/investment banking and commercial finance; investment services, including discount brokerage; and full-service banking through more than 250 offices in Latin America. FleetBoston Financial is headquartered in Boston and listed on the New York Stock Exchange (NYSE:FBF) and the Boston Stock Exchange (BSE:FBF).

CONTACT:

```
FleetBoston Financial
Alison Gibbs
617-434-2489
```

Original article: http://www.businesswire.com/webbox/bw.101000/202842566.htm

THIS TRANSCRIPT IS UNEDITED

National Committee on Vital and Health Statistics

Work Group on National Health Information Infrastructure

February 3, 1999

Hubert H. Humphrey Building
Room 705A
200 Independence Avenue, S.W.
Washington, D.C.

Proceedings By:
CASET Associates, Ltd.
10201 Lee Highway #160
Fairfax, Virginia 22030
(703) 352-0091

PARTICIPANTS:

Work Group Members:

- Don E. Detmer, M.D.
- Jeffrey S. Blair, M.B.A.
- Daniel Friedman, Ph.D.
- Richard K. Harding, M.D.
- Clement J. McDonald, M.D.

Staff:

- Mary Jo Deering, Ph.D.
- J. Michael Fitzmaurice, Ph.D.
- Rob Kolodner, M.D.
- Sandy Haydock
- Hetty Khan
- Steve Steindel, Ph.D.

TABLE OF CONTENTS

He has gotten the in the northwestern fisheries area, the environmentalists to sit down with the fishermen and all these stakeholders to come up with a way of governing that system better. So, we are fortunate that he is personally taking initiative in this area in health care because he feels that if there is a way to do this in health care and to prove how this could work, it would be very instructive.

So, for your glossary, he has coined a new term; CHAORD(?). CHAORD is an organization that combines chaos and order and blends them seamlessly so that you have the effective tension between chaos and order come together in a way that allows people's creative spirits really to come about. So, all this is abstract and theoretical, which is what I am most interested in. But, in fact, there is a very practical side of what I am here to talk to you about and that is there is a group of people that have already started to try to build a system like this for health care.

If you can see on the diagram -- that is the bubble diagram there -- this is sort of the lineage of what we have been able to accomplish so far and there are two sort of lead organizations now that are leading this charge. One is the National Health Foundation, which is an L.A.- based organization devoted to the issues that around the uninsured, led by Rita Moya(?), and the Center for Advancement for Health, which is a D.C.-based center that -- that is a group that is interested in psychosocial behaviors of health and how information sort of gets used by people.

These two organizations have come together to try to start a dialogue amongst a wide variety of organizations, ranging American Hospital Association to the American Association of Health Plans to the College of Emergency Physicians, just to name a few, to define a common vision, much like you have been doing here.

That is the other document that we have passed out here, this revised draft concept paper. It sort of gives you our sense of what our vision would be and what we are pursuing in trying to build a chaordic organization for health care.

Probably the most concrete idea we ever could get our hands around is the idea of a electronic safe deposit box, where you could your information like anything from your living will to your insurance card to your health record that would have, you know, public and private keys that could be used to give access to this information as you wish it to be given out.

And a VISA kind of organization could, in fact, help, you know, either foster the development of these electronic safe deposit boxes or actually create them themselves. We are not so much interested in the technology at this point because we see this issue fundamentally as a governance issue. There are all sorts of technology out there; Smart Cards, everything, you know. I don't even begin to know all of them myself.

What we need is an organization that can come together and agree on a rapid basis and a revolving basis, standards on operational questions that can be quickly adopted in the real world because they are benefiting people on a day-to-day basis. So, that is what we -- and, in fact, along these -- the most recent development of our outfit has been the sort of learning of a -- we have learned of a similar kind of effort at the -- that has been spearheaded by the Department of Veteran Affairs, Bureau of Indian Health Services and the Department of Defense.

I think it is fair to say that what they have learned in trying to build an electronic medical record for their folks is that it wouldn't make any sense for them to have a system that just works for them if it didn't work for everyone because their folks, you know, will move in and out of their own particular systems. So, they have understood and I think, quite correctly that we need to make this a broader societal kind of